ANONYMITY

SECURITY

TABLE OF CONTENTS

This is dedicated to all of our tender-hearted co-conspirators in this war against civilization. We'll meet in the shadows.

INTRODUCTION

Every day we see new evidence of the State's surveillance apparatus at work. Our cell phones are tracking devices; RFID chips threaten to make privacy impossible; surveillance cameras are on every street corner. Each new technological development brings with it a new encroachment into our lives and a new tool in the State's arsenal of repression. With this techno-development increasing at an exponential rate, it is difficult not to feel lost, paranoid, or caged. We live in panopticon - even if the State's eyes cannot be on us all at once, we can never be sure that we are not being watched at any given moment. This *psychic* omnipresence, coupled with the very real evidence of the surveillance apparatus's repression of agents of revolt, creates paralysis. The threat of handcuff, court room, and jail cell stay our hand.

It is impossible to ever have *perfect* security or *foolproof* anonymity. The structure of the world as a massive prison prevents our movements from ever being invisible and our actions from ever being risk-free. Our situation is far from perfect - in fact, it is frightening - but if we allow the State's surveillance to deter our revolt, we ensure the impossibility of a world free of domination. We can reject paranoia and employ *strategic anonymity* that seeks to interfere with surveillance and repression wherever possible. While we cannot become invisible, we can evade their eyes where it counts.

This project is the product of research and self-education. It grew from our desire to learn how to increase our digital anonymity and security and expanded from there. Hours of wading through manuals and websites full of technological jargon and coming back with only a basic idea of how to practically apply any of it made the necessity of an accessible, comprehensive guide apparent.

Our intention with this guide is to provide a basic outline of the following: specific ways in which you can be digitally identified and how to anonymize your internet presence; how to secure your computer and make your files or hard drive (theoretically) inaccessible to prying eyes; how to control and effectively dispose of the records of activity your computer stores; how to protect your computer from malicious processes and programs; how to

more securely use email; and other issues related to these subjects.

This guide is designed for beginners and focuses on the concrete skills; we know those were the two things we hoped for in the guides we read when we started our research. We wrote this from a subjective point-of-view; it is for our "likes," our friends we hold dear and those we have not yet met. We're poor, so most of these tools are free, and most of what isn't can be pirated. We hate techno-industrial society, so we refuse to engage in the techno-fetishism of most computer guides; we refuse to speak of any technology as "liberating" and reject idea that the internet is democratic - both because we hate alienating technologies and because we hate democracy.

We are not experts; we may be misinformed about aspects of security and anonymity and this is why with every concept, program, or activity explained, we provide an extensive list of resources for further independent research, which we encourage and recommend. The rate at which technology develops also makes information quickly outdated or impractical, so staying up to date on developments is essential to any understanding of technology and how it affects us. We know computers can be overwhelming and frustrating to learn about, but we are not hackers and, with some concerted effort, we went from a below-average knowledge of computers to a working knowledge of what affects us most about them. Anyone with some time and dedication can figure this all out, and we hope that this guide can be an aid in such research.

Future editions of this guide may be compiled as we learn more and expand our knowledge of computers and associated technology.

Toward the generalization of tactical knowledge,
Anarchists

ANONYMITY

INTRODUCTION

Everything you do on the internet can be traced back to the computer or internet connection point you use unless you obscure or anonymize aspects of your computer or connection that give away identifying information. The identifiers involve software and hardware, so an approach that takes only one of these into consideration cannot fully obscure your digital identity. In general, the more identifiers you obscure, the more difficult it will be to trace activity back to you. That said, nothing should be considered fool-proof, as a variety of errors can occur that break through the digital obscurity you set up. Anything that comes between you and what you seek access to (information, communications, whatever) increases the chance of interception; communicating face-to-face is always more secure.

The amount of effort you choose to employ in obscuring your activities depends on the nature of those activities. Innocent web browsing, accessing anarchist websites, and posting communiqués all require different levels of security. Utilizing all of these techniques in order to look up some innocuous information is a waste of time that could be spent doing more important things. On the other hand, allowing identifying information slip out when posting a communiqué could cost you your (relative) freedom. The main idea is to weigh the work required against the outcome of information leakage. If you feel a situation requires you to pull out all the stops, then do so. If it does not, do not. This is all subjective and determined by your strategy, situation, and goals. Never let striving for "perfect anonymity" deter you from action; such a thing does not exist. Remember that anonymity and security exist as precautions to keep us out of jail and free to continue attacking the institutions of domination, not as ends themselves. But also keep in mind that the State will do all it can to strip our revolt of its force; fight intelligently and cover your tracks wherever possible.

Notes: We mainly focus on Linux and Windows operating systems and Mozilla Firefox-based web browsers. We recommend switching over to Linux from Windows or Mac OSx and strongly urge everyone to uti-

lize Firefox (or a comparable browser) instead of Internet Explorer. There is a learning curve for Linux, but it can make anonymizing aspects of your hardware and software much easier, as well as protect your system from attacks. Firefox offers a variety of plug-ins and customizations that can aid in anonymizing your browsing and securing your connection, and generally avoids the holes that IE has in privacy and security if configured correctly.

We include some links for Mac OSx and Safari/Opera/Chrome/IE, so those who use those can still make use of these forms of anonymization.

The first four aspects of anonymity we explore (ISP, IP, MAC address, and session data) are the most important. While the other aspects can leak information about your browser or computer, these first four are the easiest ways to trace activity back to you or discover your past activity. We recommend focusing on these to begin with and then learning to mitigate other aspects of information leakage.

ISP

WHAT IS IT?

An Internet service provider (ISP) is a company that provides access to the internet. This is what you connect to in order to access websites, email, etc. Some examples of this are cable modems, dial-up, DSL, and wireless/wifi.

Wireless/wifi is the most important to discuss as this is the easiest to connect to in order to anonymize yourself. Wireless is either open or closed, either public or encrypted and requiring a password to access. Examples of open networks would be a public hotspot like a library or cafe, or an unsecured home network. An example of a closed network would be a home or office connection using some form of encryption.

WHY IS IT IMPORTANT?

The location of your internet connection is the final destination of any investigation of internet activity. If your activities can be traced back to an ISP, your obscurity is compromised *if you use your home connection*. Regardless of how much effort you put into obscur-

ing yourself, your information can still be grabbed at the ISP level or can be traced back to that connection. If your anonymization is compromised for any reason, you could get caught if you are using a connection that can be traced to you or anyone you associate with.

HOW TO DEAL

The hacker words of wisdom - "don't hack on your own connection" - come into play here. If you use a connection that is not related to you or anyone you associate with, even if your other attempts at anonymity fail, investigators will only be led to a dead end. In short: DO NOT DO ANYTHING FROM YOUR HOME CONNECTION THAT YOU WOULD NOT WANT INVESTIGATORS TO KNOW ABOUT.

The easiest way to anonymize your connection is to access a public wireless hotspot, such as a library or cafe. These are generally open connections and easy to access. If you feel your activities warrant it, pick somewhere with no CCTV. (Your anonymization of your IP will probably prevent your activities from ever being traced back to the wireless connection, but it better to err on the side of caution when doing anything that could threaten your freedom.) You will also want to utilize encryption (see section on internet encryption) if logging in to anything on a public connection, since someone with the right software could pick up your login information or monitor your activities. It is also vital to change your MAC address (see section on MAC addresses) to prevent logging of your hardware information in the wireless connection's routers.

Another way of getting wireless access is home networks. While this is illegal, anonymizing your hardware information makes getting caught unlikely. You can drive around with your computer looking for open wireless connections (known as wardriving).

Another possibility is to use software to hack into encrypted wireless connections. Depending on the type of connection and the password used, this can be simple. Some programs monitor the wireless connection until it has enough information to crack the encryption; others use lists of words to attempt to discover a password (dictionary attacks). While these require a bit more technical expertise, they can make finding wireless connections a lot easier.

I would recommend finding a connection away from your home for added security. This can be done by visiting wireless spots or wardriving, but can also be done in the home by using a wireless antenna. These magnify your wireless card's strength and can be used to access internet farther away from your home than you would be able to access otherwise. These can be bought online or constructed for next to no money with a few specialty cables and household products.

If you use an ISP not connected to you, you have established a major wall in any investigation of your internet activity. If you also properly alter software information and obscure your activity through anonymizers, it is unlikely your activity will be traced back to you unless a major investigation is underway.

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Internet_service_provider
http://www.howstuffworks.com/wireless-network.htm
https://secure.wikimedia.org/wikipedia/en/wiki/Wireless_LAN
https://secure.wikimedia.org/wikipedia/en/wiki/Wired_Equivalent_Privacy
https://secure.wikimedia.org/wikipedia/en/wiki/Wi-Fi_Protected_Access

Open Wireless & Wardriving
https://secure.wikimedia.org/wikipedia/en/wiki/Piggybacking_%28Internet_access%29
http://www.wi-fihotspotlist.com/
https://secure.wikimedia.org/wikipedia/en/wiki/Wardriving
http://www.wardriving.com/
http://kismac-ng.org/
http://www.netstumbler.com/
http://www.kismetwireless.net/

Antennas
http://www.radiolabs.com/Articles/wifi-antenna.html
http://www.turnpoint.net/wireless/cantennahowto.html
https://secure.wikimedia.org/wikipedia/en/wiki/Cantenna
http://cruftbox.com/cruft/docs/cantenna.html

Cracking
https://secure.wikimedia.org/wikipedia/en/wiki/Wireless_cracking
http://www.kismetwireless.net/
http://www.aircrack-ng.org/

IP

WHAT IS IT?

Your IP (Internal Protocol) address is a string of numbers that allows you to send and retrieve data over an internet connection. It consists of four numbers, each of which contains one to three digits, separated by a single dot. Each number ranges from 0 to 255. An example would be 78.125.1.209. This number identifies the location, ISP, and technical details of your connection. It is comparable to a house's street address.

WHY IS IT IMPORTANT?

An unobscured IP will lead investigators directly to your connection. If you did not use a foreign internet connection, this leads right to you. Even if you use another ISP to connect to the internet, obscuring the IP will complicate investigation and, depending on type of obscurity and the persistence of the investigators, probably prevent them from even figuring out the connection you used. By anonymizing your IP, you are throwing up another wall for investigators.

HOW TO DEAL

There are a variety of ways to obscure your IP. For the purposes of this guide, we are going to explore proxies and TOR - two free and relatively simple ways to increase anonymity. We also include links to VPN

services and SSH tunnels for those who want to investigate alternatives.

Proxies are systems or websites that allow you to run your connection through theirs. Rather than connect to the website you wish to connect to, you connect to the proxy server, which then connects to the website you are trying to access. The logs of the website you are trying to access will then show the proxy's IP address rather than yours.

Proxies can be website-based and list-based. With website-based proxies, you access the website and type the URL of what you wish to access and it tunnels the connection through the proxy website. While these generally work consistently and are faster than other proxies, the anonymity they offer is negligible. They could keep extensive logs of what you view, which could be a major problem if you use them frequently. Many are also US/UK based and therefore do not contain the added frustration of international investigation for the feds. List-based proxies can be gleaned from various internet lists and entered in your browser's configuration (generally under network settings in your browser's options). These are generally slower and often do not work, but some offer the benefit of international proxies, which may complicate investigations.

In general, we do not recommend the use of these "one-hop" proxies if you wish to protect privacy. Whoever operates the proxy server will have access to anything you view, which is dangerous if it is a honeypot operation (the state operating proxies to catch criminals and hackers) or if they maintain logs. If you are using your home network to connect to a proxy, your ISP will have logs showing that you connected to the proxy's IP at a specific time and your activities can be discovered if the proxy server maintains logs. Some also add something called x_forwarded_for headers that send your actual IP to the websites you connect to. I would only recommend using these one-hop proxies if there are no other choices and if you are connected to something other than your home network. Always check if the proxy is working by using an IP checking site. You can also look into proxy chaining, which allows for connection to multiple proxies and will mitigate some of these risks to a degree.

TOR is a better choice for anonymity. It is a network of proxies run by volunteers with the explicit purpose of maintaining anonymity. With TOR, your connection goes through three proxies. You con-

nect to TOR and each of the three proxies (nodes) you access encrypts your data. No individual node can know what you are connected to and who you are. The third node decrypts the data and accesses the website, sending the information back through the proxies encrypted. While nothing is foolproof, TOR provides a strong anonymity for its users.

The drawbacks of TOR are its speed and its exit node. TOR, like many proxies, is very slow, but the anonymity it achieves is worth the time it takes if you want to keep your browsing private. The unencrypted exit node is a more serious problem. The operator of the third node could see your data (website accessed, login information) if you do not encrypt the connection (see section on browser encryption). While this will not personally identify your connection, it could compromise any accounts you log in to, so encrypt!

TOR also offers a simple TORbutton for Firefox that allows for easy use, a portable browser that can be installed on a flash drive so you don't have to install TOR on your computer and can use it on any computer, and is present in some LiveSystems for security and portability (see section on LiveSystems).

One note of caution: do not do something stupid like logging into a personal email address or posting personal information using the same proxy or TOR configuration you use for doing anything sketchy. People have been caught this way, so use common sense.

LINKS

General
http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm
http://www.webopedia.com/TERM/I/IP_address.html

Proxy basics
https://secure.wikimedia.org/wikipedia/en/wiki/Proxy_server
http://www.webopedia.com/TERM/P/proxy_server.html
http://whatismyipaddress.com/using-proxies

Proxy lists
http://samair.ru/proxy/
http://nntime.com/

Proxy chaining
http://www.freeproxy.ru/en/free_proxy/faq/how_create_proxy_chaining.htm
http://www.hackingtricks.in/2011/01/how-to-create-proxy-chain-proxy.html

IP checkers
http://whatismyipaddress.com/
http://www.whatismyip.com/
http://browserspy.dk/ - checks a variety of info your browser gives away

SSH
https://secure.wikimedia.org/wikipedia/en/wiki/Tunneling_protocol
https://secure.wikimedia.org/wikipedia/en/wiki/Secure_Shell
http://www.chiark.greenend.org.uk/~sgtatham/putty/
http://www.openssh.com/

VPN
en.wikipedia.org/wiki/Virtual_private_network
https://www.openvpn.net/

TOR
https://www.torproject.org/
https://www.torproject.org/projects/torbrowser.html.en
https://addons.mozilla.org/en-US/firefox/addon/torbutton/
https://secure.wikimedia.org/wikipedia/en/wiki/Tor_(anonymity_network)

MAC Address

WHAT IS IT?

The MAC (Media Access Controller) address - also known as the hardware address or physical address - is a number that uniquely identifies the piece of hardware connecting to a network. An example of hardware with a MAC address would be your laptop's wireless card. MAC addresses are 12-digit hexadecimal numbers, written in the format of MM:MM:MM:SS:SS:SS. The first half of the address identifies the manufacturer of the adapter, the second is the serial number assigned by the manufacturer.

WHY IS IT IMPORTANT?

The MAC address specifically identifies your computer. If you access the internet, the router may log your MAC address and maintain that log. If investigators were to read the logs of a router you accessed (say, a public wifi from which a communiqué was sent), and then compare that address with the MAC address of your computer's wireless card (say, confiscated in a raid), you'd be connected to your activity while using that router's connection. If the MAC address is not changed, there is the possibility of your activity being traced back to you if investigators are persistent or lucky enough.

HOW TO DEAL

In order to avoid this, you need to change your MAC address. The ease of doing this depends on your operating system. If you do not wish to learn these ways, you can use MAC spoofing software to automate the process. Whether you do that or spoof the MAC yourself, always double check that the MAC was indeed changed before starting your internet activity.

LINUX

One of many advantages of Linux is the simplicity of spoofing MAC addresses. It is only a matter of entering a command into the terminal and creating a new address. Programs exist for Linux that will generate and spoof MAC addresses automatically as well.

MAC CHANGE IN LINUX

1. Click Terminal
2. Type: ifconfig 'device name' down" (with the name of your networking device in place of 'device name')
3. Type: ifconfig 'device name' hw ether 00:11:22:33:44:55 (with the numbers being what you wish to change your MAC address to)
4. Type "ifconfig 'device name' up"
5. Check MAC address with ifconfig

WINDOWS

In Windows, the MAC address can be changed in the registry or by configuring the hardware properties. These methods take a bit of work, but should alter your MAC address if executed correctly. Be careful when altering registry or configuring hardware; we would advise reading up on these ways of changing MAC addresses more before you attempt them. Alternatively, there are programs that automate the process in Windows.

TO VIEW MAC ADDRESS

1. Start
2. Run
3. Type: cmd
4. Type: ipconfig/all
5. Look for your adapter, its MAC address will be listed as Physical Address

REGISTRY

1. Go to Start
2. Run
3. Type: regedit
4. Navigate as follows:

[HKEY_LOCAL_MACHINE>>SYSTEM>>CurrentControlSet>>Control>>Class>>{4D36E972-E325-11CE-BFC1-08002BE10318]

You will see a lot of options like 000, 001, etc under {4D36E972-E325-11CE-BFC1-08002BE10318}. Here you will have to choose the option which matches your current MAC address. For example, if my current MAC is 00-18-8B-BA-DD-55; I will choose 0018 since the first four

HEX numbers of the MAC are 00-18.
5. Right click the Network Address and choose Modify
6. In a new window which pops up, write a new MAC under Value data.
7. Click OK. Disable and then enable your adapter and check your new adapter MAC in Command.

HARDWARE PROPERTIES

This will vary depending on the version of Windows you are using and its form of navigation.

1. Start
2. Control Panel
3. Network and Internet
4. Network and Sharing Center
5. In the side bar, click Change adapter settings
6. Find the adapter whose MAC address you wish to change, right click and click Properties
7. Go to the Advanced Tab OR click the Configure button and then go to the Advanced tab
8. Look for Network Address, MAC Address, or Physical Address
9. Change
10. Check MAC address in Command

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Mac_address
http://www.wikihow.com/Find-the-MAC-Address-of-Your-Computer

Spoofing
http://www.technitium.com/tmac/index.html
http://www.irongeek.com/i.php?page=security/changemac
http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer
http://standards.ieee.org/develop/regauth/oui/oui.txt

SESSION DATA/BROWSER SETTINGS

WHAT IS IT?

Session data is any log saved on your computer when you do access websites or do work online. Session data includes cookies, cache, history, saved forms and passwords, and form and search history. In addition to this, some browser settings, such as domstorage and geolocation, either save browsing information or identify your location.

A cookie is information a website saves on your hard drive so it can recall information about you at a later time. There are two types of cookies, session and persistent. Session cookies are erased when the browser is closed. These are stored in temporary memory and are not retained after the session is terminated. Persistent cookies, or stored cookies, are stored on a user's computer until they expire or are deleted. These cookies are used to collect information, such as what you view online or website preferences.

Local Shared Object or Flash Supercookie differs from the browser cookie. The supercookie is based in the Flash application and is stored in a different location than browser cookies. These are difficult to locate or uninstall.

History is a list of web sites visited, categorized by date.

Cache, also known as the temporary internet files folder, is a container of files from visited websites. This allows for faster display of websites, as the display is retrieved from the cache, rather than from the site's web server.

Form and search histories are saved logs of information entered in website forms or search bars. Saved passwords are any passwords you have set to be saved for easy access in your web browser.

DOMstorage is a storage feature for organizing persistent data. It is built into browsers and enabled by default.

Geolocation is a browser setting that allows for geographically-sensitive date to be suggested in searches and queries when you access websites. For example, searching "movie times" in Google will bring up a list of theaters near your perceived location.

WHY IS IT IMPORTANT?

Most of these mechanisms store information about what you view, when you view it, and any data you enter while using the internet. This

leaves a trace - or a large pool of evidence if you never clear this data - of your activities. Even if you go all-out with anonymity, if you don't curtail your browser's information storage, your computer will be filled with logs of your online activity. If you're engaging in projects of subversion and revolt, having this information stored on your hard drive could get you locked up.

HOW TO DEAL

It is not difficult to curb your browser's retention of data. A few changes to settings and an add-on or two will go a long way in keeping this information from ever being saved in the first place, and if it is saved, from being deleted in a timely manner. Besides the solutions offered, there is the possibility of running a browser from a LiveSystem, which will prevent all of this information from ever being saved on your hard drive, as LiveSystems run from RAM only (see section on LiveSystems). Most of the following is geared toward Firefox-based browsers. We recommend switching to one of these because of their customizations and concern for security. Some links will be included to help with other browsers.

Your first move should be to edit your browser's privacy settings. Uncheck any option that remembers information such as search or form history, download history, and browsing history. Turn off cookies, or set them to expire when you close your browser. Set browsing history, cache, cookies, site preferences, download history, offline data, and saved passwords to clear when the browser is closed.

You can also disable some of these manually. Type "about:config" into the URL. In the filter bar, type what you wish to edit, such as cache or cookies. Toggle settings such as "browser.cache.disk.enable" to false, and set the value of preferences such as "browser.cache.disk.capacity" to 0. Check online for various ways to edit your browser's preferences this way to achieve better privacy.

While we advise doing BOTH of the above by default, the easiest way to make it so your browser never saves the information to begin with is to browse in private mode. Most browsers have this capability, and it makes it so your computer does not keep any record of your browsing history. Always use private mode.

Doing the above should prevent the better known threats to

privacy from being a concern, but there are other specifics that should be altered as well, such as Flash cookies, geolocation, and DOMstorage.

To disable DOMstorage, type "about:config" into the URL. In the filter bar, type "dom.storage". Toggle "dom.storage.enabled" to false, set "dom.storage.default_quota" to 0. This will disable domstorage.

To disable geolocation, type "about:config" into the URL. In the filter bar, type "geo.enabled". Toggle "geo.enabled" to false. This will disable geolocation.

To delete LSO/Flash supercookies, your best bet is to download an add-on called BetterPrivacy. Enable the settings to delete Flash cookies on browser exit, delete cookies on application start, delete cookies by timer, delete Flash default cookie, or any other settings you wish to use to curb Flash cookies. This will also delete the DOMstorage file if you ask it to.

Links

Private Mode
https://support.mozilla.com/en-US/kb/Private%20Browsing
http://www.meabi.com/how-to-enable-private-browsing-in-internet-explorer-9/
http://www.switchingtomac.com/tutorials/safari/private-browsing-in-safari/
https://www.google.com/support/chrome/bin/answer.py?answer=95464

DOMstorage
https://secure.wikimedia.org/wikipedia/en/wiki/Web_Storage
http://securitygarden.blogspot.com/2010/08/how-to-disable-dom-storage-cookies.html

Geolocation
https://www.mozilla.com/en-US/firefox/geolocation/

LSO flash cookie
https://secure.wikimedia.org/wikipedia/en/wiki/Local_Shared_Object
http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/
https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/
http://netticat.ath.cx/BetterPrivacy/BetterPrivacy.htm

REFERER

WHAT IS IT?

The referer (sic), also known as the referring page, is the URL of the page the link was followed from. If you click a link, the website the link leads to will see the page the link was clicked on, as the referer is part of the HTTP request the browser sends to the website's server.

WHY IT IS IMPORTANT?

Referers can give a website information about your activities because they tell what page you were on when a link was clicked. This can be linked with your IP to gain information about your browsing.

HOW TO DEAL

There are a few programs or add-ons that help to control the referer.

In Firefox, an add-on called RefControl will allow you to customize the referer each site sees. You can customize a specific referer for a site, or you can create a default referer setting for all sites. RefControl can send no referer, send the root of the site you are accessing as the referer, and can create custom referers that say anything. We recommend changing the referer to the root of the site or blocking it.

Another option is to use Privoxy, which is often packaged with TOR. If you set Privoxy settings to do so, they will alter various aspects of your browser identification. Like RefControl, Privoxy can be set to

hide the referrer, set it as the root site, and change it to any web address.

LINKS

http://www.privoxy.org/
https://addons.mozilla.org/en-US/firefox/addon/refcontrol/

USER AGENT

WHAT IS IT?

A user agent is a string of information a web browser sends to a website to identify itself. This fits a website's content for that particular browser or operating system. The user agent consists of six components: application name, application version, compatibility flag, browser name and version, operating system, and any extensions installed. Each of these depends on the particulars of your computer (whether you have Windows or Linux, Internet Explorer or Firefox, for example).

An example of a user agent would be:

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Mozilla designates the application name. 5.0 is the application version. Compatible is the compatibility flag. MSIE 7.0 is the version token. Windows NT 6.0 is the operating system.

WHY IS IT IMPORTANT?

Disguising your user agent is important if you wish to prevent websites you view from knowing your particular operating system and web browser. This information, if accessed by investigators, could aid an investigation by narrowing down the possibilities. If your user agent corresponds to one engaged in illegal activities, you could be linked to those activities.

HOW TO DEAL

To check your user agent and see if it has changed, type "about:" into the URL. Always double check to make sure your changes worked.

There are a few ways of changing a user agent.

There is a Firefox add-on called User Agent Switch-

er that will automate the process for you. This is very simple and convenient, but be sure not to use the same user agent, even if it is fake, for activities you do not wish to be connected.

Another option is Privoxy, which will allow you to alter your user agent. You set up Privoxy as a local proxy and it will filter your connect through it, changing the user agent to whatever you set it as.

To manually change your user agent, type about:config into the address bar. Right click somewhere and in the menu that comes up select New -> String. Enter "general.useragent.override" as the preference name. In the window for the string value, enter the user agent you want the browser to use.

You can find lists of user agents to switch to online. Certain pages may cease to work if you change the browser or operating system, so you may just want to glean the particulars from it and leave the basic browser and operating system information intact. If the website you wish to access doesn't fail to work because the user agent does not match your browser, then by all means change it to anything you'd like. Common browsers and operating systems are best for increased obscurity.

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/User_agent

User agent checker
http://whatsmyuseragent.com/

Switching user agent
http://www.labnol.org/software/change-google-chrome-user-agent-string/4566/
http://johnbokma.com/mexit/2004/04/24/changinguseragent.html
https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/
http://www.privoxy.org/

List of strings
http://www.useragentstring.com/pages/useragentstring.php

802.11 NICKNAME

WHAT IS IT?

The 802.11 nickname is an obscure feature of the wireless connection that sends your hostname (your computer's name) to the access provider.

WHY IS IT IMPORTANT?

If you access, for example, public wifi that is later investigated, and your 802.11 nickname is logged there, this can be matched up with your computer's name. This will show that you access this wifi at a specific time and can connect you to activities you took part in while on that connection.

HOW TO DEAL

The best defense against this is to choose a common machine name. Some examples might be default, computer, PC, home, and user. It would be difficult to prove that you did something on a public wifi connection if the only evidence is that both your computer and the computer in the logs are named "computer."

In Windows, there is no easy way to change the 802.11 nickname. If you don't already have a common computer name, we would recommend reinstalling your operating system and choosing a more common name, or better yet, switching to a Linux OS.

In Linux, open terminal.
Enter [root@machine ~/dir]# iwconfig ath0 nickname "whatever name you want"

Another way is the following: Type "gksudo gedit /etc/ hostname". Change value and save (but make sure you write down the old value first if you wish to change it back). Then type "gksudo gedit / etc/ hosts" and change that as well.

There are also ways to edit the hostname in GUI (Graphic User In-

terface). This varies depending on the Linux distribution and release you are using, but you should be able to find the particulars by using the following as a guidepost, or by researching how to do it in your particular distribution.

Go to System -> Administration -> Networking. In Network Settings, under the General Tab, click Host Settings. Under Hostname, type the computer name you want. Save changes and restart your computer.

LINKS

http://billstclair.com/matrix/ar01s03.html
http://lifehacker.com/?_escaped_fragment_=343768/change-a-computer-name-in-linux#!343768/change-a-computer-name-in-linux

SCRIPTS

WHAT ARE SCRIPTS?

Scripts are attributes of websites that allow certain aspects of those websites to run or function. Video, audio, and even some basic aspects of a webpage require scripts.

WHY IS IT IMPORTANT?

While many scripts simply allow you to view material on a website, not all are benevolent. Some scripts are used for advertisement, behavioral tracking, and accessing your computer. These can be serious compromises to your security and anonymity.

HOW TO DEAL

The main problem when dealing with scripts is that disabling them may restrict the capabilities of your browser. Content you need to access may be blocked. However, there are ways of dealing with this that allow you to pick and choose what you allow to run.

Your first option is to manually disable scripts. This will completely prevent the disabled scripts from running.

To disable JavaScript in Firefox:

Tools -> Options -> Content -> Uncheck "Enable JavaScript"

To disable other scripts in Firefox:
Tools -> Add-ons -> Turn off Java, JavaScript, Flash, Silverlight in Extensions and in Plug-ins

There are also add-ons which allow you to pick and choose which scripts you run or which you block. The Ghostery add-on for Firefox will list the scripts running on a page and allow you to choose which to block should they come up on other websites. This allows you to choose which to block, but does not automatically prevent scripts from running, which can be a problem if you do not already have the unwanted scripts for a page blocked.

NoScript is a valuable add-on for Firefox. By default, it blocks all active content, including Flash, Silverlight, JavaScript, and Java. You can allow certain scripts temporarily or permanently and also add scripts to a permanent block list. If used correctly, this significantly reduces the risk of exploitation by malicious scripts. As a warning, it neuters your web experience and requires a few more clicks on websites if content is blocked - this seems a small price to pay for the benefits, however.

Adblock, an add-on that blocks advertisements (banner ads, commercials in videos, etc.), is useful as well. Subscribe to the basic lists and most advertisements will be blocked.

One major source of tracking and behavioral analysis is Google. Many websites run Google scripts (Adsense, Analytics, Recaptcha, Apis, etc.), and Google keeps logs indefinitely, so avoiding this tracking is advisable. An add-on called GoogleSharing will filter your requests from most Google services through a proxy to anonymize the results and keep Google from tracking your online behavior by anonymizing your IP, HTTP headers, and User Agent. The service maintains no logs, encrypts connections, and was developed by an anarchist. (Note: This will only offer basic anonymity and is therefore best for everyday browsing - disable this and use TOR when you are doing sensitive work online.) You can

also use Scroogle, a website that allows anonymizing of Google searching.

LINKS

Scipt-blocking
http://noscript.net/
http://www.ghostery.com/
https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

Google alternatives/proxies
https://ssl.scroogle.org/
http://www.googlesharing.net/
https://addons.mozilla.org/en-us/firefox/addon/googlesharing/

ENCRYPTION

WHAT IS ENCRYPTION?

For this section, we are focusing on encryption of browsing via HTTPS/SSL encryption. There are other forms of encryption, some of which offer better security, which can be further explored by visiting websites in the links section.

Encryption is a way to secure the sending or receiving information over the internet. When you access a website, the sent and received information travels in plain-text from your computer, along networks, to the server you are accessing. Anyone in the middle of these connections (your ISP, the server you are connecting to, eavesdroppers) can view the information. Encryption secures this information by scrambling the data, turning it from plain-text to a (generally) undecipherable code. HTTPS encryption is represented by a little lock in the corner of your browser window, as you may have seen when logging in to email or bank accounts.

WHY IS IT IMPORTANT?

Encryption is vital to security. Unencrypted data is like a postcard: anyone between the sender and receiver can view it. SSL encryption, while it does not offer perfect security, is a simple way to improve

the security of a connection significantly, protecting from digital eavesdropping. If you are using a public wireless connection, this is even more vital, since it is impossible to know who is also using the connection. (There are a variety of tools which enable the theft of user names and passwords from unencrypted connections with little effort.)

HOW TO DEAL

SSL encryption is simple. Rather than typing"http://" into the address bar, type "https://". Not all websites allow SSL encryption, but many do.

The Electronic Frontier Foundation has a Firefox add-on, HTTPS Everywhere, that automatically encrypts a variety of popular websites such as Google search, Twitter, PayPal, Wikipedia, Facebook, etc. You can also write your own rule sets to allow automatic encryption of other websites. This is useful for adding security to everyday browsing and log-ins.

LINKS

SSL/TLS/HTTPS
https://secure.wikimedia.org/wikipedia/en/wiki/Transport_Layer_Security
https://secure.wikimedia.org/wikipedia/en/wiki/HTTP_Secure
https://www.eff.org/https-everywhere

SSH
https://secure.wikimedia.org/wikipedia/en/wiki/Secure_Shell
http://www.openssh.org/
http://www.chiark.greenend.org.uk/~sgtatham/putty/

SECURITY

INTRODUCTION

Computer security has two main aspects: protecting your system from attacks and securing your data. The former involves protecting your computer from viruses, malware, keyloggers, rootkits, and various other threats. The latter focuses on protecting your data from anyone who gains access to your computer, by encrypting data, managing logs, and securely deleting files.

Securing your computer and data puts a wall up against potential investigators or digital infiltrators. The amount of information investigators mine from your computer in the case of hacking or a raid depends solely on the time and effort you put into the security of your system. We strongly advise dedicating sincere effort to this, as it is often the only thing keeping your computer safe from the state's prying eyes.

SECURE DELETION

WHAT IS SECURE DELETION?

When you delete a file by emptying it from the recycle bin, the file is not actually deleted. The computer has merely marked the space the file takes up as "empty" so new data can be written over it; the file itself remains until it is written over. Secure deletion, on the other hand, writes random data over a file multiple times, effectively deleting the original file.

WHY IS IT IMPORTANT?

Files you delete on your computer remain there, invisible to you. If this is sensitive data and your computer is confiscated, this can be a problem, as computer forensics can uncover the deleted files, sometimes even if they have been written over by another file. To prevent your deleted files from resurfacing, it is necessary to securely delete the files.

HOW TO DEAL

There are a variety of programs and commands which will automate the process of secure deletion, which we have pro-

vided in the links. In Linux, you need to get the shred program (sometimes it comes with a distributions default software package); the command ((((((((((INSERT COMMAND)))))))))) shreds the files. For Windows, you will need a shredding program.

How effective the shredding of files is depends on which algorithm is used. In general, the more passes an algorithm makes over the file, the better the chances of wiping all traces. The more passes, the longer the shredding will take; but we recommend using Guttman algorithm, as this passes over the file 30 or more times. Algorithms that claim to be those used by Department of Defense or other government agencies are mostly hype and make only a few passes over the file.

In addition, most shredding software allows you to shred your computer's free disk space. This writes over the entirety of the free space on your computer's hard drive, securely deleting any remnants of files that are being stored there. We recommend shredding free disk space weekly using a strong algorithm. Combined with a practice of secure deletion, this should prevent forensics specialists from accessing the files, except perhaps with the use of expensive microscopes, which is possible but unlikely.

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Data_remanence
https://ssd.eff.org/tech/deletion
https://secure.wikimedia.org/wikipedia/en/wiki/Gutmann_method

Programs/Processes
http://www.heidi.ie/eraser/
http://www.piriform.com/ccleaner
http://bleachbit.sourceforge.net/
http://www.fileshredder.org/
http://srm.sourceforge.net/
https://secure.wikimedia.org/wikipedia/en/wiki/Srm_%28Unix%29

https://secure.wikimedia.org/wikipedia/en/wiki/Shred_%28Unix%29
http://www.freesoftwaremagazine.com/columns/shred_and_secure_delete_tools_wiping_files_partitions_and_disks_gnu_linux
http://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html

VIRUSES AND MALWARE

WHAT ARE THEY?

A virus is a program which, when saved on your computer, replicates by making copies of itself. It often causes damage to or interferes with the operation of your computer. Viruses often operate without the user being aware, sometimes attaching to programs or replacing them. They can spread to other computers via any transfer of the infected file(s).

Malware is malicious software, designed to secretly infiltrate a system without the user's consent. It is often intrusive and interferes with a computer's operation or invades a user's privacy. Examples of malware are spyware, adware, worms, and trojan horses.

WHY IS IT IMPORTANT?

Viruses and malware can inturrupt the proper functioning of a computer, damage or destroy files, and erase entire hard drives. Beyond the annoyance of a ruined computer, anonymity and security are threatened. Anything you do on your computer is compromised when malware or viruses interfere; state agencies seeking information could create and install the virus and malware in order to compromise your machine.

HOW TO DEAL

Anti-virus programs and anti-malware programs will mitigate the threat of viruses and malware. However, the security these offer depends on the quality of the program, user security settings, and updates. We have included a variety of free and freeware programs in the links section; pay programs can also be pirated. It should be noted that anti-virus/malware programs are based solely on reaction to

threats. Software is updated when threats are found, which can sometimes be too late if the virus/malware is already on your computer.

Firewalls will further help prevent intrusion by malware, viruses, and a variety of other threats. These prevent unauthorized access to your computer from outside sources which do not meet specified security criteria. Much like anti-virus/malware software, however, the strength of this depends upon user settings and updates.

Some general tips for protecting yourself from viruses

- Only download files or open email attachments you know the contents of.
- Keep your anti-virus and firewall fully updated.
- Set programs to moderate or strict settings.
- Make sure programs are running at all times.
- Do a full scan for viruses and malware weekly.

Another option is to use a Linux operating system. Linux is more secure by default, most viruses and malware are designed for Windows and Mac, and security updates are much more comprehensive because Linux is open source. While editing firewalls in Linux can be difficult for most (the writers of this booklet included), there are programs such as Firestarter which simplify the process. Linux also offers an anti-virus program called KlamAV, which we recommend using to scan any files being sent to a Windows machine, as Linux can be a carrier of Windows viruses but be uneffected.

LINKS

(We are mostly including freeware programs. You can also pretty easily pirate other programs: http://www.thepiratebay.org)

General
http://ubuntuforums.org/showthread.php?t=510812
http://www.schneier.com/

Anti-Viruses
http://www.avast.com/free-antivirus-download
http://free.avg.com/us-en/homepage
http://www.avira.com/en/avira-free-antivirus
http://www.cloudantivirus.com/en/
http://www.clamav.net/lang/en/

Anti-Malware
http://www.safer-networking.org/index2.html
http://www.lavasoft.de/software/adaware/

Firewalls
http://free.agnitum.com/
http://www.online-armor.com/
http://www.comodo.com/home/internet-security/firewall.php
http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm
http://www.fs-security.com/

Intrusion Detection Systems & Access Control
https://secure.wikimedia.org/wikipedia/en/wiki/Linux_Intrusion_Detection_System
http://www.snort.org/
https://help.ubuntu.com/community/AppArmor
http://www.ossec.net/

KEYLOGGERS

WHAT IS A KEYLOGGER?

A keylogger is a program or piece of hardware that records every keystroke you make on your keyboard. It creates a log, which it then sends to a specified receiver. Keylogger hardware is a small, battery-powered plug that connects the keyboard to the computer; it often resembles the keyboard's plug. Hardware keyloggers generally need to be physi-

cally accessed in order to obtain logs. Keylogger software, on the other hand, allows for remote monitoring. This is often installed via spyware.

WHY IS IT IMPORTANT?

Obviously, keylogging is a threat to security. Keyloggers can intercept passwords, user names, browsing history, and anything typed on the computer. This could compromise encryption keys, browsing anonymity, and email accounts, and also give investigators a play-by-play look at user activity.

HOW TO DEAL?

The information on viruses and malware apply to keyloggers as well. Firewalls, anti-virus and anti-malware programs, intrusion detection systems, and discretion in regard to downloads will all reduce the chance of keyloggers being installed on your machine. LiveSystems, discussed in a later section, also bypass keylogging software by only accessing the RAM of a machine.

Virtual keyboard programs can also thwart keyloggers by giving a graphic keyboard, often encrypted and randomized, to type on by clicking letters. Password vaults are another option (see section on passwords).

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Keystroke_logging

Anti-keylogging programs
http://www.qfxsoftware.com/download.htm
http://free-anti-keylogger.com/
http://dewasoft.com/privacy/kldetector.htm
http://www.maxsecuritylab.com/dataguard-anti-keylogger/download-anti-keyloger.php
http://www.spyshelter.com/download.html

Virtual Keyboards
https://secure.wikimedia.org/wikipedia/en/wiki/Virtual_keyboard

http://library.gnome.org/users/gnome-access-guide/stable/gok.html.en
http://florence.sourceforge.net/english.html
http://www.microsoft.com/enable/training/windowsxp/usingkeyboard.aspx
http://www.lakefolks.org/cnt/
https://launchpad.net/onboard
https://addons.mozilla.org/en-US/firefox/addon/keylogger-beater/
http://networkintercept.com/vrkeyboard.html
http://myplanetsoft.com/free/mouse-only-keyboard.php

ROOTKITS

WHAT IS A ROOTKIT?

A rootkit is software that allows for privileged access to a computer without the knowledge of the user. These are often designed to actively mask their presence by manipulating the functioning of an operating system. Rootkits allow for ongoing intrusion and circumvent authentication.

WHY IS IT IMPORTANT?

As with spyware and viruses, rootkits sacrifice your anonymity and security. They allow a remote user to manipulate your operating system and bypass most security setups by subverting the software. This compromises anything you do on your computer.

HOW TO DEAL

The best protection, as always, is to prevent rootkits from being installed in the first place. Practicing good digital security and discretion about what you download will go a long way in helping prevent rootkits from being installed on your computer. Rootkits generally require some access to your computer's administration to gain access to your computer. You can help prevent this by restricting access to root (in Linux) or administrative privileges (in Windows), encrypting parts or all of your hard drive, using strong passwords (see

section on passwords), and never giving root access or passwords to anyone who does not need them or who you do not trust completely.

Due to the hidden nature of rootkits, detection is difficult, especially for users without deep knowledge of computers. Some programs, including some anti-malware programs listed in the malware section, have some ability to detect rootkits. Linux has a program called chkrootkt designed for this exact purpose; Windows has comparable programs. Besides those options, there is only analyzing your computer's memory dump, which requires experience.

If you think you have been compromised by a rootkit, reinstallation of your operating system may be the easiest or only way of dealing with the problem. Try to search around for help online first.

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Rootkit

Detection & Removal
http://www.sophos.com/en-us/products/free-tools/sophos-anti-rootkit.aspx
http://www.lavasoft.de/software/adaware/
http://www.f-secure.com/en/web/home_global/protection/internet-security/overview
http://www.chkrootkit.org/
http://www.rootkit.nl/projects/rootkit_hunter.html
http://www.avast.com/free-antivirus-download
http://www.ossec.net/
http://www.usec.at/rootkit.html

PASSWORDS

WHY IS IT IMPORTANT?

The strength of a password, your protocol around passwords, and your use of passwords can all determine the security of your computer, encryption, and user/email accounts. Simple passwords, loose lips, and indiscriminate password entry on unknown computers can all compromise your encryption keys and user accounts.

HOW TO DEAL

Some tips on passwords

- NEVER tell anyone your password.
- Make it at least 15 characters long. The longer a password is, the more difficult it is to crack with dictionary attacks, which quickly cycle through lists of words, entering each as the pass word until it cracks it.
- Never include your name, user name, or anything related to your life.
- Never make it a word found in the dictionary, as this is easily cracked by dictionary attacks.
- Make new, distinct passwords for each account.
- Include all of the following: uppercase letters, lowercase letters, numbers, and symbols. This complicates any attempt to crack the password via dictionary attacks.
- Make the password the first letters of a line of a song or poem. For example, “Do they owe us a living? Of course they fucking do!” becomes “d7OU@L?0<TfD!”
- Change passwords. The frequency depends on your ideal level of security.
- If you are logging in on a computer you are not 100% sure of the security of, using a virtual keyboard and/or a LiveSystem can allow you to use the computer without sacrificing your password to potential threats.
-There are programs that allow for encrypted storage of passwords and encryption keys, putting them all under one master password. This can also be accomplished by pasting password in a Notepad file and storing it

in an encrypted volume. For increased obscurity, insert random information around the password to confuse anyone who may gain access to the file.

LINKS

General
http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/
http://www.wikihow.com/Build-a-Strong-Password

Password managers
http://keepass.info/
http://lifehacker.com/software/geek-to-live/geek-to-live--secure-your-saved-passwords-in-firefox-154099.php

ENCRYPTION

WHAT IS IT?

Encryption allows for a scrambling of data. Where once a file was easily accessible in plain text, now it is ciphered and rendered unreadable - unless the encryption is broken or the password obtained. In this section, we are focusing on file and full disk encryption. (For information on browser encryption, see Part I – Anonymity and Browsing; for email encryption, see the section on email.)

Full disk encryption encrypts at the hardware level - your entire hard drive. This means that, without the key, no one can access the hard drive's contents, even if the hard drive is removed. After you enter your password once on startup, full disk encryption automatically encrypts all files on your hard drive as they are created, and decrypts them when they are accessed.

File/volume encryption encrypts a specific file or volume containing multiple files.

WHY IS IT IMPORTANT?

Encryption is the final wall between your files and those who wish to access them. Encrypting data prevents unwanted access to files, as long as the encryption is not broken and the password is protected.

With every raid on anarchists by the state, we hear of journals, phone books, and computers being confiscated and used to form a case. The computer is confiscated, and all of the files contained on its hard drive become evidence; journals and phone books construct a reasonably clear view of a person's networks and activities. Encryption could prevent this.

Instead, let's say an encrypted computer is confiscated. The owner encrypted their important files - phone numbers, encryption keys, personal writings. Investigators hit a brick wall and are unable to access these files. Barring any traces of files on the computer, the owner may be able to keep their files secret (even more so if they practiced other security and anonymity methods, or encrypted their entire hard drive!). Encryption is vital. Encrypt everything.

HOW TO DEAL

Full Disk Encryption

Full disk encryption can be done at the installation of an operating system (some Linux distributions offer an option), or later on using software. As this differs depending on the operating system or software, we are avoiding a step-by-step guide, but including a variety of links to other programs or guides.

It is worth noting here that full disk encryption has one flaw which someone with computer expertise can exploit to gain access to your hard drive. With full disk encryption, a small part of your hard drive must by unencrypted, so it can decrypt the rest of it. This section can be manipulated to gain access to your hard drive in a cold-boot attack. A possible way to avoid this is to put the decrypting portion on a flash drive and hide it. We have provided some resources for how to do this.

Encrypted Volumes

Encrypted volumes create a sort of "cabinet" for your folders and files. All contents of the encrypted volume are unreadable unless the vol-

ume is decrypted. A popular program for creating/mounting encrypted volumes is TrueCrypt, which we are using as the basis for this section.

With encrypted volumes, you create the volume and then mount it and decrypt it to access the files contained within. There is also the possibility of using a hidden volume. With a hidden volume, you have two passwords for the encrypted volume - one for the outer volume (dummy volume), and one for the inner volume (hidden volume). If you are (il)legally forced to give the password to your volume, you can give up the outer volume and no one will know that there is an inner volume present, thus protecting your files and offering plausible deniability.

First you create an outer volume. We recommend using a strong algorithm such as AES, as stronger algorithms are much more difficult to crack. You are given a small box with randomly generated numbers, which you swirl your mouse around in to create the encryption - the longer you do this, the more difficult the encryption will be to break. Then you are given the option of adding some files to the outer volume. This increases the illusion of it being the real volume if you are forced to give up your password. You then repeat the process, creating the inner volume. It is best to memorize the inner volume password, as this is where you will be storing files you want hidden.

Some Tips on Encryption

- Always use strong passwords. Your encryption is only as secure as the password used to protect it.
- Be careful of keyloggers. Use a virtual keyboard, LiveSystem, or a password manager.
- Choose a strong algorithm. Truecrypt even allows for multiple algorithms.
- Create your volume on a flash drive. These can be physically hidden, which may elude investigators or other thieves. This also allows for portability if you keep a portable version of TrueCrypt on the flash drive.
- Use in coordination with LiveSystems to prevent traces of files from being stored on your hard drive.
- When in doubt, encrypt. The less information investigators can potentially mine from us, the better. Think about whether or not you'd want something to be used in court or seen by your enemies. If not, encrypt it.

LINKS

General
http://www.schneier.com/
https://secure.wikimedia.org/wikipedia/en/wiki/Disk_encryption

Programs and Processes
http://www.maximumpc.com/article/howtos/how_to_encrypt_your_entire_hard_drive_the_easy_way_using_truecrypt
http://www.wisegeek.com/how-do-i-encrypt-files.htm
https://secure.wikimedia.org/wikipedia/en/wiki/Comparison_of_disk_encryption_software
http://www.truecrypt.org/
http://www.truecrypt.org/hiddenvolume

Potential problems
https://secure.wikimedia.org/wikipedia/en/wiki/Cold_boot_attack
https://secure.wikimedia.org/wikipedia/en/wiki/Full_disk_encryption#The_boot_key_problem

LINUX

WHY LINUX?

Linux as an operating system is more secure than Windows by default. This is due to the fact that it is open source: its code is freely accessible. Windows is a proprietary operating system: its updates come from Windows developers. Linux, being open source, can be maintained by anyone. This generally means that security flaws are patched much quicker, and the system is therefore more secure. In addition, Windows and Mac operating systems are generally the target of attacks, leaving Linux immune to many viruses and other malicious software.

Linux also offers a wide array of free programs and options, many of which aid greatly in security and anonymity. As shown in previous sections, it is much easier to accomplish certain tasks (changing

MAC address or computer nickname) in Linux. Many Linux distributions also come with an option of full disk encryption on installation.

DRAWBACKS

The main drawbacks of Linux are the learning curve and incompatibility.

Most people are familiar with Windows and/or Mac and how those operating systems function. Linux can prove more difficult for those unfamiliar with how it works. One major difference is that much of Linux is based in the Terminal. With those familiar with Graphic User Interfaces (GUIs), this command-line way of operation can be confusing. One must know the lines to type in order to achieve a goal. Commands can be learned, however, and many Linux programs offer a GUI alternative to Terminal.

Incompatibility can sometimes be a problem for specific programs; some programs are just not compatible with Linux. There are three solutions to this problem. First, Linux can run Wine, which packages various basic Windows programs so the user can create Word files or Excel spreadsheets. Second, Linux has comparable programs to a majority of Windows-and-Mac-only programs, such as Scribus for InDesign and GIMP for Photoshop. The main complaint is that these are sometimes less powerful than their Adobe counterparts. Third, the creation of a Windows LiveSystem will allow you to run Windows off of the computer's RAM while still maintaining Linux as your computer's operating system.

CONCLUSION

Linux is the way to go for security and anonymity. It simplifies actions which are more complex in Windows and offers much stronger security by default. The drawbacks are easily overcome with some research and familiarization with Linux and its functions.

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Linux
http://ubuntuforums.org/

Distributions
http://www.ubuntu.com/
http://fedoraproject.org/
http://www.opensuse.org/en/
http://www.redhat.com/
http://www.knoppix.com/
http://www.debian.org/

LIVESYSTEM

WHAT IS IT?

A LiveSystem is a portable operating system that can boot from a CD or flash drive. The two varieties of LiveSystems are LiveCDs and LiveUSBs. LiveUSBs differ in that they are (depending on the distribution) able to save changes to the operating system, where LiveCDs are not. These operating systems run from the computer's RAM.

WHY DOES IT MATTER?

LiveSystems can aid in security and anonymity. By running on the RAM, LiveSystems can avoid leaving traces of activity on a computer, and bypass the computer's hard drive and whatever malicious software is installed there. This is especially useful when using a public computer or any computer you do not maintain yourself, as these may contain keyloggers, viruses, and other programs which compromise your privacy. By leaving no traces, LiveSystems allow you to avoid the logs and snippets of files left all over your computer by programs.

Some LiveSystems are specifically designed to aid anonymity and security and include services such as TOR, anonymous and encrypted messaging and email programs, encryption software, virtual keyboards, wireless hacking software, etc.

HOW TO DEAL

Creating a LiveSystem depends on the service you choose, but mostly just involves downloading and installing/burning. We have

included useful distributions in the links section.

When choosing a system, look for:

- An encryption program (so you can access encrypted files without leaving traces on your hard drive)
- Anonymizing software such as TOR, MAC changers, various Firefox extensions
- Email client which supports encryption & email encryption program
- Wireless hacking programs (if needed)
- Virtual keyboard

In general, it would be wise to use a LiveSystem when:

- Accessing encrypted data. (This will prevent logging of encrypted file names, contents, etc. It may also bypass keyloggers and other threats to your encryption security.)
- Working with sensitive files. (Same reason as the above.)
- Using a public computer or a friend's computer. (The security of these machines may be lacking and they may contain malicious software.)
- Doing sensitive research. (Another way to prevent traces of your internet activity from being left on your hard drive. A LiveSystem with anonymity software will also help you anonymize your internet presence.)

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Live_CD
https://secure.wikimedia.org/wikipedia/en/wiki/Live_USB
https://secure.wikimedia.org/wikipedia/en/wiki/List_of_live_CDs
https://secure.wikimedia.org/wikipedia/en/wiki/Comparison_of_Linux_distributions#Live_media

Livesystems designed for anonymity
https://tails.boum.org/ (Highly recommended! TOR, FireGPG & Claws Mail, HTTPS Everywhere, Aircrack-ng, Pidgin preconfigured for Off-the-Record Messaging, onBoard virtual keyboard, lots of open

source software.)
https://www.privacy-cd.org/ (Cannot connect to the internet. For viewing encrypted material.)
http://www.mandalka.name/privatix/ (TORbutton)
http://www.sabayon.org/ (Allows default use of TOR on startup.)
http://www.polippix.org/ (TOR, MAC changer, GnuPG, traffick sniffer)

General Linux Livesystems
http://www.livecdlist.com/
https://www.knopper.net/knoppix/index-en.html
http://www.debian.org/distrib/
https://fedoraproject.org/en/get-fedora
http://www.kubuntu.org/

EMAIL

WHAT IS IT?

With the proliferation of cellular phones and social networking sites, it seems people are using email less and less to communicate. Still, email offers a quick and easy way to communicate; the development of a secure practice of emailing can benefit our networks greatly.

WHY IS IT IMPORTANT?

Like all communication, email can be intercepted. Considering that emails travel over many networks, secure and unsecure, they should not be considered a safe form of communication. What authorities learn from this interception varies depending on the contents and form of the email. If a message contains sensitive information, it could lead to raids, arrests, or investigations. It is also a simple way of network mapping: seeing with whom someone is communicating, how frequently, and about what. Security and/or anonymity practices in this context can limit the risks of email communication.

HOW TO DEAL

How you go about communicating via email depends on your needs. In general, you can seek anonymity or security, though it is possible to achieve both. Anonymity would involve practicing anonymity when accessing email (see Part I – Anonymity and Browsing), anonymous remailers, or the use of draft folders. Security would involve email encryption and/or use of cryptolects (secret languages). Again, it is possible to attempt both security and anonymity - for instance, by using coded language in anonymously sent emails.

Remailers

Anonymous remailers take a message and forward it to a recipient without revealing the point of origin. Different types of remailers maintain different strategies of anonymity, privacy policies, etc. The level of anonymity essentially depends on the individual remailer, so we advise doing some research before choosing one to use. Remailers generally operate in a similar way to proxies. They take a message, strip it of originating IP and headers, and forward it to a recipient. Some include more hops, forwarding it to one node, which then forwards to another node, etc., before arriving at its final destination.

There are a few general types of remailers

- Pseudonymous remailers, which simply give a pseudonym to the sender in place of your actual email, and allow the recipient to reply.

-Cypherpunk remailers, which strip away the sender's address, send the message encrypted to the remailer, which decrypts it and sends it to the receiving address. These allow you to chain remailers, adding more hops to the process and increasing anonymity. These generally do not keep logs. The recipient cannot reply to the message.

-Mixminion remailers, which use a program to anonymize mailing. These allow replies.

-Web-based remailers, which are websites that allow you to send anonymous messages. These are simple to use, but provide less anonymity than real remailers.

Drafts

Another option is to use the draft folder of an email to communicate. This is said to avoid NSA screening of emails, as the messages are never sent, only stored in the draft folder. The positive aspect of this is that, unlike remailers, it does not require special software, only attention paid to anonymity when accessing the account. The downside is that the anonymity of the account requires all with access to have strong anonymity practices; unless you trust the ability of the others to practice anonymity when logging into the account, this is a bad idea. Also, if the account is compromised, the contents of your communication may be compromised as well.

Regardless of whether you are using remailers or draft folders to communicate, it is best to follow the following guidelines:

- Never plan actions over email (or any digital communication for that matter). Only do this face-to-face. Use these communications at most as a way to plan meet-ups.
- Use vague or coded language. Never put your name or personal information in an anonymous email. Never give the date/time/location of meet-ups in plain language. Pre-establish code names for places, times, days of the week, etc.
- Utilize anonymity (see Part I – Anonymity and Browsing) when accessing email or using remailers to resend email.
- Don't keep emails unless you need them. Delete emails regularly.
- Once the email account has served its purpose, clear all emails and delete the account.

PGP Encryption

Emails are sent in plain text. This means that anyone operating servers your email travels through (or monitoring those servers by sniffing packets) can read the contents of your email. PGP can mitigate this harm and protect the contents of your email from prying eyes.

The basics of PGP are the private key and the public key. You publish your public key, a series of letters and numbers, making it available to anyone who you wish to receive encrypted email from. You keep the private key to yourself, preferably storing it encrypted in some form

(see section on file encryption). When someone wishes to send you an encrypted email, they use your public key to encrypt it; then, only your private key can decrypt it. To everyone else - servers, investigators and other snoops - it just looks like jumbled numbers and letters.

To configure PGP in Thunderbird

To begin with, you'll need Mozilla's Thunderbird email program, an extension for it called Enigmail, and GNUPG software (see links).

After you have done this, open Thunderbird. In the menu, open the OpenPGP option and go to Preferences. Where it says to point to your GNUPG binary, click Browse and find the GNUPG program you have installed.

Now you generate your public and private keys. In the OpenPGP menu, choose Key Management. Then, in the Generate menu, choose New Key Pair. Select an email address you want to generate the key for and click Generate Key. After a few minutes, your keys will be generated.

You will also be able to generate a revocation certificate, which will invalidate a public key if the private key is compromised. We recommend generating this and saving it encrypted.

When sending an email, you compose it as usual in Thunderbird. A key in the lower right of the window will allow you to encrypt and to sign a message (this proves it is you by signing with your private key). If these turn green, they are activated.

To search for someone else's PGP key, choose Key Management under the OpenPGP menu. In the Keyserver menu, choose Search. Search by name or email address and add the person's public key to your key manager. This will allow you to encrypt email to that person.

How secure is PGP?

Encryption is typically very difficult to crack. There is evidence that the FBI (and comparable foreign agencies) is currently not able to decrypt modern PGP. There is the possibility that complex computers owned by the NSA, for example, may be capable of breaking PGP, but no evidence of this exists.

It should be noted that the Fifth Amendment (protection

from self-incrimination) has allowed suspects to refuse to give away passwords. Still, it is naive to assume investigators will grant you this right, and it is best to prepare yourself. Keep your mouth shut, always.

On the other hand, breaking the encryption or forcing a suspect to reveal a password is often not necessary. Investigators have used keystroke loggers and software in order to obtain encryption keys and passwords. The only preventative measure against this is to harden your system against such attacks and practice good security behaviors (See Part II - Security).

The more ubiquitous the use of PGP, the more invisible our communications will be. Encrypt everything.

(NOTE: We see many anarchist groups and individuals who use Gmail as their email provider. We urge strongly against this. Gmail scans all emails to provide advertisements fitted to users' interests. Combine this with the amount of information Google has on you via searches, behavior tracking through scripts, etc, and a serious privacy problem arises.

Gmail has handed over data to investigators in the Mt. Hope Infinity trial, showing Google's true face as a willing participant in the state's repression apparatus. Evade Google (see section on scripts). Use an email service such as Riseup, which is maintained by anti-authoritarians, emphasizes security, and has actively opposed investigators where Google has collaborated.)

LINKS

General
https://secure.wikimedia.org/wikipedia/en/wiki/Anonymous_remailer
https://secure.wikimedia.org/wikipedia/en/wiki/Cypherpunk_anonymous_remailer
https://secure.wikimedia.org/wikipedia/en/wiki/Mixmaster_anonymous_remailer
https://secure.wikimedia.org/wikipedia/en/wiki/Nym_server
http://www.emailprivacy.info/remailers
http://anonymous.to/tutorials/anonymous-remailers/

http://mixmaster.sourceforge.net/
http://mixmaster.sourceforge.net/faq.shtml
http://www.autistici.org/en/stuff/user_howto/anonymity/man_re-mailer.html
https://i2pbote.net/

ENCRYPTION

General information
https://secure.wikimedia.org/wikipedia/en/wiki/Email_encryption
https://secure.wikimedia.org/wikipedia/en/wiki/Public-key_cryptog-raphy
https://secure.wikimedia.org/wikipedia/en/wiki/Pretty_Good_Privacy
http://lifehacker.com/180878/how-to-encrypt-your-email
https://secure.wikimedia.org/wikipedia/en/wiki/Mozilla_thunderbird
https://secure.wikimedia.org/wikipedia/en/wiki/Enigmail
http://web.archive.org/web/20070205025633/dudu.dyn.2-h.org/nist/gpg-enigmail-howto

Programs and Processes
http://www.gnupg.org/
http://www.openpgp.org/
https://www.mozillamessaging.com/en-US/thunderbird/
http://www.openpgp.org/resources/downloads.shtml
https://enigmail.mozdev.org/home/index.php.html
https://addons.mozilla.org/en-us/thunderbird/addon/enigmail/

SESSION DATA

WHAT IS IT?

Session data consists of the various traces of activities and files left on your computer. Examples of this include system logs, accessed programs, thumbnails, recent documents, searches, browser data, and temporary files.

WHY IS IT IMPORTANT?

Even if you practice good security and anonymity, traces of files on your computer can give you away. Logs can contain evidence of your activities that can potentially compromise your security; thumbnails and recent documents lists can show what files you have created, stored or accessed; browser data can give a map of what you do online. Data of this sort must be managed and curtailed if you want to keep your behavior private.

HOW TO DEAL

There are a variety of ways in which to manage session data on your computer. Secure deletion and shredding free disk space (see section on secure deletion) help to eliminate traces left by deleted files. Deleting browser session data (or not saving it at all) reduces or eliminates traces of your internet activity saved on your computer (see section on session data/ browser settings). You can also use a LiveSystem (see section on LiveSystems), which will bypass your hard drive and prevent logs from being created in the first place. It is a good idea to use LiveSystems when accessing files or programs you do not want to leave traces of on your computer. Encrypting your hard drive will secure log files as well (see section on encryption).

Still, there are other traces left in various places on your computer that need to be sorted out and deleted. Linux, again, has advantages over Windows in that most Linux distributions clear the /tmp folder on boot, do not have a registry, and have specific places in which logs are stored. Most temporary files are stored in /tmp and /var/log.

In Linux, logs can be managed with the logrotate tool. Some deletion programs, such as BleachBit, can also be installed on Linux.

In Windows, some logs can be manually deleted.

1. Click Start and go to the Control Panel
2. Click System and Maintenance/Security and go to the Administrative Tools section
3. Click View Event Logs
4. Here you can right click various logs and clear them.

Another option is to use a program that deletes program and system data. These generally allow for secure erasure as well. The capability of these programs depends on the individual software, but they generally examine your computer for specific programs or logs and give you the option of deleting them. This is useful for clearing out recently used programs and files, temporary files, thumbnails, browser data, cache, Office logs, system restore points, search history, system logs, etc. Always set these programs to use algorithms with multiple passes (see section on secure deletion).

We recommend using multiple means of deletion to ensure proper management of logs and session data. Manually delete logs, run cleaning programs, secure delete, regularly shred free disk space, encrypt your hard drive, and do not save browser data.

LINKS

Linux
http://linuxcommand.org/man_pages/logrotate8.html
http://linuxers.org/howto/howto-use-logrotate-manage-log-files
http://www.thegeekstuff.com/2010/07/logrotate-examples/

Windows
http://www.wikihow.com/Delete-your-Usage-History-Tracks-in-Windows
http://msdn.microsoft.com/en-us/library/twdecbsx.aspx
http://www.ehow.com/how_5900134_delete-windows-log-files.html

Programs
http://bleachbit.sourceforge.net/ (Linux & Windows)
http://www.piriform.com/ccleaner (Windows)

METADATA

WHAT IS IT?

Metadata are identifying attributes embedded in a document. For example, Microsoft Office embeds data in any document you create, such as computer name, company name, etc. What we will focus on, as we see these as most pertinent to anarchists, are Office files and images.

WHY IS IT IMPORTANT?

Metadata can give away your identity. In the case of Office files, your computer name and other machine information is given away. In the case of images, camera information, time, and even geographical coordinates can be embedded. If you want these documents or images to remain anonymous (in the case of a photo of an action or riot, a submission to an anarchist zine, a communiqué), you have to remove the metadata.

HOW TO DEAL

Microsoft Office

Office embeds name, computer name, initials, company name, and revision information in all documents. While it is advisable to use generic, non-identifiable names for your hardware and software (see section on 802.11 nicknames), any embedded data can link you to the file.

To remove metadata from an Office document, you do the following:

1. Right click the document and click Properties
2. Go to the Details tab and click Remove Properties and Personal Information
3. Select all and remove the data.

You can also remove data before the file is saved by doing the following:

1. Click Tools
2. Click Options
3. Go to the Security tab and check Remove personal information from this file on save

OpenOffice
1. Click File
2. Click Properties
3. Uncheck Apply User Data & also click Delete

PDFs
1. Open PDF file in Adobe Acrobat (you must use Acrobat; Adobe Reader cannot be used to edit PDF files).
2. Display Document Properties using File | Document Properties. If it's not already the active tab, move into the 'Description' tab).
3. Delete any undesirable text present in the 'Author', 'Subject,' or 'Keywords' fields.
4. Move to the "Custom" tab and do the same.
5. File|Save As to the same name to overwrite, or save to a different filename, if desired.

Images

Digital cameras and photo editors automatically record metadata. The easiest way to remove this metadata is to download a scrubbing program. We have included links to a few of these for Linux/MacOS and Windows.

LINKS

Office files & PDFs
http://lawyerist.com/how-to-quickly-and-easily-remove-meta-data/
https://techpaul.wordpress.com/2009/06/15/how-to-remove-metadata-from-your-files/
http://www.microsystems.com/resources/wordtips/wordtip003.php

Exif data on images

http://www.geosetter.de/en
http://www.exiferaser.com/
http://www.exifpilot.com/
http://www.relliksoftware.com/exifdatechanger/
http://www.sno.phy.queensu.ca/~phil/exiftool/

http://www.photome.de/

DESTRUCTION OF HARD DRIVE

WHY IS IT IMPORTANT?

If you have information on a hard drive or flash drive that absolutely needs to be destroyed, you may choose to completely destroy the drive. Good security practices should make this unnecessary, but in the rare case that you have extremely sensitive data that needs to be totally eliminated, we are including a few tips on how to do this.

HOW TO DEAL

1. Run a file shredding program and wipe the entire drive. This will overwrite the data and destroy most traces of files. The more times this is done, the less the chance of data retention.
2. Run a powerful magnet over the drive, thus demagnetizing it and further distorting the contents. You can find these magnets in the hard drives of junk computers, some stereo speakers, etc.
3. Burn/smash the hard drive.
4. Take the broken parts and dispose of them in separate places, preferably putting some distance between the various parts. Practice counter-surveillance techniques if you think you are being followed.

It is possible that, if a section is found, powerful microscopes could still access parts of files or data. However, the above steps should make the hard drive itself difficult to find, and complicated or impossible to access if its parts are found.

LINKS

https://secure.wikimedia.org/wikipedia/en/wiki/Darik%27s_Boot_and_Nuke
http://www.heidi.ie/eraser/
http://www.piriform.com/ccleaner
http://bleachbit.sourceforge.net/
http://www.fileshredder.org/

RESOURCES

DIGITAL
HackThisZine
https://www,hackbloc.org
Electronic Frontier Foundation
https://www.eff.org
Surveillance and Counter-surveillance Guide
http://anti-politics.net/distro/2009/warriorsecurity-read.pdf
Snitchwire
http://www.snitchwire.blogspot.com/
NGOinabox
https://security.ngoinabox.org/
Ubuntu Forums
http://ubuntuforums.org/
ExitTheMatrix
http://billstclair.com/matrix/
Security Self-defense
https://ssd.eff.org/
Activist Security
http://www.activistsecurity.org/
Green is the New Red
http://www.greenisthenewred.com/
Hacker10
http://www.hacker10.com
North Carolina Piece Corps
https://ncpiececorps.wordpress.com/
2600 Magazine
http://www.2600.com/

BOOKS/MAGAZINES
Beat the Heat – Katya Komisaruk
The Art of Deception – Kevin Mitnick
The War At Home – Brian Glick